NELSON MANDELA UNIVERSITY

STAFF LAPTOP STANDARDS GUIDELINES AND GOVERNANCE FRAMEWORK

ICT Services

Document Owner	ICT Services
Document Type	Institutional Guidelines and Governance Framework
Version	1.0
Effective Date	1 June 2026
Review Cycle	Annual technical review; governance review as required
Applies To	All University-funded staff laptop acquisitions and lifecycle management

1. Introduction

Nelson Mandela University requires a consistent, secure and sustainable approach to the acquisition, allocation, configuration, support and lifecycle management of staff laptops. These Guidelines and Governance Framework establish the institutional standards and decision-making controls applicable to University-funded staff laptops.

The framework is intended to move laptop provisioning away from ad hoc purchasing towards a controlled, standardised and auditable model that supports service delivery, hybrid work, cybersecurity compliance, asset accountability and responsible use of University resources.

2. Purpose

The purpose of this document is to define the minimum technical standards, role-based laptop categories, security requirements, procurement controls, lifecycle principles, asset-management responsibilities and exception processes that govern staff laptop provisioning at Nelson Mandela University.

3. Objectives

- Standardise staff laptop acquisition and deployment across the University.
- Ensure that laptop allocation is based on legitimate business need and workload requirements rather than personal preference.
- Provide fit-for-purpose devices that support academic, administrative and operational requirements.
- Ensure compliance with the University's endpoint security and enterprise-management baseline.
- Improve procurement efficiency, supportability and lifecycle planning.
- Reduce total cost of ownership and support complexity arising from non-standard or consumer-grade devices.
- Strengthen asset accountability, audit readiness and transparent exception management.

4. Scope and Application

These Guidelines apply to all University-funded staff laptop purchases, including new allocations, replacements, refreshes, standard builds, accessories, warranties, pooled devices and project-funded staff devices.

Smartphones and tablets are outside the scope unless explicitly approved as an alternative computing device. Specialist research workstations and high-compute environments should be managed through an appropriate specialist standard.

5. Guiding Principles

Business need: Laptop allocation must be driven by the requirements of the role and workload category.

Standardisation: University-funded laptops must comply with approved technical, security and support standards.

Security by design: Devices must satisfy institutional endpoint security requirements before deployment.

Value for money: Procurement decisions must consider fitness for purpose, supportability, warranty, lifecycle and total cost of ownership.

Technology neutrality: Specifications should define required capabilities and permit compliant enterprise-grade alternatives.

Lifecycle sustainability: Refresh and replacement decisions must be lifecycle-based, condition-aware and budget-conscious.

Asset accountability: All devices remain University assets and must be registered, assigned, traceable and auditable.

Controlled exceptions: Non-standard requests must be formally motivated, costed, assessed, approved and recorded.

6. Laptop Standardisation Framework

ICT Services will maintain role-based laptop tiers. The appropriate tier is determined by workload, mobility, software and operational requirements.

Tier / Category	Primary Users	Typical Workload	Target Lifecycle
Tier A - Standard Productivity	General staff; routine administrative and academic use	Email, M365, ITS/CRM, browser systems, Teams	5 years
Tier B - Professional / Power Productivity	ICT staff, analysts and power users	BI tools, heavy spreadsheets, reporting, light virtualisation	5 years
Tier C - Mobile Executive / Premium (Levels 1-5)	Executives and high-mobility roles	Travel, presentations and extensive virtual meetings	5 years
Tier D - High Performance	Developers, GIS, data, engineering and specialist users	Containers, IDEs, data modelling and specialist workloads	5 years, subject to workload assessment
Tier E - Rugged / Field	Security, estates, maintenance and field personnel	Harsh environments and field operations	5 years

7. Minimum Technical Standards

7.1 Standard Staff Laptop Baseline

- Enterprise/business-class laptop
- Intel Core Ultra 5 / AMD Ryzen 5 or equivalent approved enterprise processor
- 16 GB RAM
- 512 GB NVMe SSD
- 14-inch or 16-inch FHD display
- Wi-Fi 6 or newer and Bluetooth 5+
- 720p/1080p camera suitable for hybrid work
- Windows 11 Professional
- Minimum 3-year onsite warranty
- Standard enterprise ports and docking compatibility

7.2 Executive / Premium Laptop Baseline

- Enterprise/business-class premium laptop
- Intel Core Ultra 7 / Ultra 9 or AMD Ryzen 7 / 9
- Minimum 32 GB RAM
- Minimum 1 TB NVMe SSD
- High-resolution 2.5K/OLED touchscreen display preferred
- Premium lightweight design, normally not exceeding approximately 1.5 kg
- Wi-Fi 6E / Wi-Fi 7
- 1080p FHD camera with enhanced collaboration capability
- Advanced biometric security and TPM 2.0

- 3-5 year onsite warranty

Executive or premium specifications are role-based institutional standards and must not be treated as an automatic entitlement based solely on personal preference.

8. Security and Compliance Standards

All staff laptops must support the University's endpoint security baseline, including:

- TPM 2.0 and Secure Boot
- Full-disk encryption
- Multi-factor authentication (MFA)
- University-approved endpoint protection
- Mobile Device Management / enterprise endpoint management
- Device compliance and posture reporting
- Strong password or PIN authentication and automatic screen locking
- Asset tagging and registration within the University's asset-management environment

A device that cannot support the approved enterprise-management and endpoint-security controls must not be procured as a standard staff laptop.

9. Laptop Allocation Guidelines

Laptop allocation must be based on legitimate operational requirements. The line manager must confirm the business need and role requirements, while ICT Services validates the appropriate tier and technical standard.

- Tier A should be the default for routine academic and administrative productivity.
- Tier B requires a demonstrable professional or power-productivity workload.
- Tier C applies to approved executive or high-mobility roles requiring premium portability and collaboration capability.
- Tier D requires specialist workload justification and ICT validation.
- Tier E applies where field or environmental conditions require ruggedised capability.

10. Procurement and Standardisation Requirements

- All University-funded laptops must be sourced against ICT-approved specifications and through applicable SCM/Procurement processes.
- ICT Services must validate technical compliance before procurement.
- SCM/Procurement must obtain or process compliant quotations against the approved specification and supplier arrangements.
- Consumer-grade or unsupported devices must not be procured as standard institutional laptops.
- ICT Services should maintain an approved catalogue or reference specification that can be updated as technology and market conditions change.

11. Standard Accessories and Warranty

ICT Services should maintain an approved catalogue of accessories such as power adapters, docking stations, laptop bags, headsets, keyboards and mice. Accessories should be allocated according to operational requirements and should not automatically accompany every device where they are unnecessary.

The standard warranty requirement is a minimum three-year onsite manufacturer warranty. Extended warranty arrangements may be considered where appropriate for higher-value or specialist devices.

12. Lifecycle and Replacement Framework

The standard institutional lifecycle for staff laptops is five years. Reaching the lifecycle threshold initiates a replacement assessment and does not, by itself, create an automatic entitlement to replacement.

ICT Services should consider the following when determining replacement priority:

- Device age and warranty status
- Hardware condition and repair history
- Performance and workload suitability
- Operating-system and application compatibility
- Security compliance and supportability
- Economic viability of continued repair or support
- Operational risk and business criticality
- Availability of approved budget

High-performance or specialist devices may be considered for earlier refresh where workload intensity, supportability, security or operational requirements justify accelerated replacement. Such cases must be assessed and validated by ICT Services.

13. New Appointments and Replacement Requirements

Departments must identify laptop requirements for new appointments as early as reasonably possible. The line manager must confirm the role and workload requirement, and the budget owner must confirm funding where the allocation is not covered by an approved institutional replacement programme.

14. Damage, Loss, Theft and Negligence

14.1 Accidental Damage

Accidental damage includes unintentional incidents arising during normal use, such as dropping a laptop, liquid spills or damage caused by power surges. ICT Services will assess whether repair is economically viable. Where repair is uneconomical, the applicable University insurance and financial processes should be followed.

14.2 Negligence

Negligence refers to failure to exercise reasonable care in safeguarding University-issued equipment, including leaving devices unattended in public spaces, exposing equipment to unsafe conditions or recurring incidents of avoidable damage. Such cases should be subject to formal management review before any liability is determined.

14.3 Loss or Theft

Loss or theft must be reported promptly in accordance with applicable University security, asset and insurance processes. ICT Services must update the asset record and take appropriate endpoint-security actions.

15. Loan and Spare Laptop Management

ICT Services should maintain a controlled pool of standard laptops to support onboarding, warranty repairs, temporary equipment failure, short-term project requirements and emergency replacement. Loan devices remain University assets and must be issued, tracked and returned through the approved asset-management process.

16. Non-Standard Devices and Exception Management

Exceptions may be considered only where an approved standard device cannot meet a legitimate operational requirement, including macOS/Linux-native workflows, specialist engineering or GPU workloads, accessibility requirements or field-use constraints.

Every exception request must include:

- Business justification
- Workload description
- Required applications/software
- Reason the approved standard is unsuitable
- Proposed specification
- Cost comparison or cost differential
- Budget-owner confirmation
- Security implications and ICT recommendation

ICT Services and the budget owner must approve non-standard requests. Exceptions that affect the security baseline must also be reviewed and approved by Information Security. ICT Services must maintain an exception register.

17. ICT Asset Management and Accountability

- Every laptop must be asset tagged and recorded in the University's asset-management environment.
- Each issued laptop must be linked to an identifiable user and cost centre.
- Asset records must be updated when equipment is transferred, replaced, returned or disposed of.
- University-issued laptops must be returned on resignation, transfer, contract end, replacement or institutional request.
- Periodic verification and lifecycle reporting must support inventory accuracy and audit readiness.

18. Governance Process

The standard provisioning workflow is:

1. Department identifies a business need for a new, replacement or refreshed laptop.
2. Line manager confirms the operational requirement and workload category.
3. Budget owner confirms funding availability where required.
4. ICT Services validates the approved tier, technical baseline and catalogue alignment.
5. SCM/Procurement processes compliant sourcing against the approved specification.
6. Non-standard requirements are escalated through the exception process.
7. ICT Services configures, secures, asset-tags, registers and issues the approved device.
8. The device remains subject to asset, security, warranty and lifecycle monitoring.

19. Roles and Responsibilities

Role	Responsibility
ICT Services	Defines and maintains standards and the approved catalogue; validates requests; configures and supports devices; enforces endpoint controls; oversees lifecycle management and exceptions.
End-user Department	Confirms business need, nominates the user, supports asset accountability and motivates non-standard requirements.
Line Manager / Budget Owner	Confirms operational need, approves appropriate expenditure and ensures accountable use of issued equipment.

SCM / Procurement	Procures compliant devices from approved suppliers and ensures sourcing and quotation compliance.
Information Security	Defines/approves endpoint-security controls and reviews security-impacting exceptions.
End User	Exercises reasonable care, complies with ICT requirements and returns University equipment when required.

20. Financial and Budgetary Governance

These Guidelines establish governance standards and do not constitute blanket approval of funding. All laptop acquisitions, refreshes and replacements remain subject to approved budgets and applicable University financial and procurement processes.

- Future acquisitions must align with approved standards and available budgets.
- Standardisation should be used to improve procurement efficiency and reduce support overhead.
- Lifecycle information should inform medium-term capital and operational replacement planning.
- Non-standard devices that increase cost require explicit business justification and approval.
- Large-scale replacement funding requests should be supported by a quantified replacement schedule and asset-age profile.

21. Monitoring, Compliance and Reporting

ICT Services should maintain appropriate governance reporting on:

- Laptop population by tier
- Asset age profile and devices approaching replacement
- Endpoint-security compliance
- Warranty status and repair trends
- Approved exceptions
- Loan/spare pool utilisation
- Procurement expenditure and lifecycle forecasts
- Asset returns and outstanding accountability actions

22. Review and Maintenance of Standards

The governance principles in this Framework should be reviewed when institutional, regulatory or operational requirements change. Technical reference specifications and the approved catalogue should be reviewed at least annually, or earlier where changes in processor platforms, operating-system requirements, cybersecurity standards, supplier availability or market conditions warrant revision.

23. Effective Date and Governance

This Framework becomes effective upon institutional approval. ICT Services is the custodian of the Staff Laptop Standards Guidelines and Governance Framework and is responsible for maintaining the technical reference specifications, approved catalogue, baseline controls, exception register and lifecycle oversight.

Annexure A - Laptop Tier Reference Framework

The following reference framework provides a governance baseline. Detailed model-specific specifications should be maintained separately by ICT Services so that they can be updated without revising the full governance document.

Tier	CPU / Memory	Storage	Display / Mobility	Typical Use
A - Standard	Ultra 5 / Ryzen 5; 16 GB	512 GB NVMe	14/16-inch FHD	Routine academic/admin productivity
B - Professional	Higher approved business CPU; memory according to workload	512 GB+ NVMe	Business-class display	BI, reporting, power productivity, light VMs
C - Executive	Ultra 7/9 or Ryzen 7/9; 32 GB minimum	1 TB NVMe minimum	High-resolution touchscreen; lightweight	Executive mobility and collaboration
D - High Performance	Specialist CPU/RAM/GPU according to validated workload	According to workload	According to specialist requirement	Development, GIS, engineering, data workloads
E - Rugged / Field	Enterprise platform appropriate to field requirement	According to workload	Rugged/field-suitable	Security, estates, maintenance, field use

Annexure B - Exception Request and Approval Framework

Required Information	Description
Business requirement	Describe the operational need and why a standard device cannot meet it.
User / role / department	Identify the intended user, role and responsible department.
Workload and applications	List specialist software, processing, GPU, operating-system or accessibility requirements.
Proposed specification	Provide the requested configuration and relevant support/warranty requirements.
Cost comparison	Compare the proposed exception with the appropriate approved standard.
Budget confirmation	Confirm the responsible budget and approval authority.
ICT assessment	Confirm technical necessity, supportability and lifecycle implications.
Information Security assessment	Required where the request changes or affects the institutional security baseline.
Decision and record	Record approval/rejection, conditions, approvers and exception-register reference.

Document Control and Approval

Document Custodian	ICT Services
Approval Authority	Capital Resource Allocation Committee
Effective Date	1 June 2026
Next Review Date	30 July 2027
Version	1.0